UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/729,209	12/05/2003	Jean-Pierre Duplessis	MS306247.01/MSFTP552US	9483

27195 7590 04/21/2008

AMIN. TUROCY & CALVIN, LLP
24TH FLOOR, NATIONAL CITY CENTER
1900 EAST NINTH STREET
CLEVELAND, OH 44114

EXAMINER	
TRAORE, FATOUMATA	

ART UNIT	PAPER NUMBER
2136	

NOTIFICATION DATE	DELIVERY MODE
04/21/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docket1@thepatentattorneys.com
hholmes@thepatentattorneys.com
osteuball@thepatentattorneys.com

Office Action Summary	Application No.	Applicant(s)	
	10/729,209	DUPLESSIS ET AL.	
	Examiner	Art Unit	
	FATOUMATA TRAORE	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 January 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10,12,13,15-17,19,21 and 22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10, 12-13, 15-17, 19, 21-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed January 31, 2008. Claims 1-6, 8, 12, 15, 19 and 21 have been amended; Claims 11, 14, 18 and 20 have been cancelled; Claims 1-10, 12, 13, 15-17, 19, 21, and 22 are pending and have been considered bellow.

Response to Arguments

2. Applicant's arguments with respect to claims 1-10, 12, 13, 15-17, 19, 21, and 22 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 1, 12, 21 and 22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the claims recite the limitation of "wherein the identification of the encryption type is based at least in part upon a failure of a portion of authentication sequence of the available wireless network or exceeding a time threshold during the authentication sequence of the available wireless network" It is unclear to the examiner how applicant is performed the step of identifying the encryption

type. The examiner suggests including a step of providing more details on how the identification of the encryption type is determine. Appropriated correction is required.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 1-10 are drawn to a computer program per se(component), which the applicant has defined in the specification (page 4, lines 15-30) to encompass a software and a software in execution in execution (computer program). A computer program is not a series of steps or acts and this is not a process. A computer program is not a physical article or object and as such is not a machine or manufacture. A computer program is not a combination of substances and therefore not a compilation of matter. Thus, a computer program by itself does not fall within any of the four categories of invention. Therefore, Claims 1-10 are not statutory.

7. Claim 19 is drawn to a data packet. Data packet is an electronic transmission signal. The Office considers an electronic signal to be a form of energy. Energy is not a series of steps or acts and this is not a process. Energy is not a physical article or object and as such is not a machine or manufacture. Energy is not a combination of substances and therefore not a compilation of matter. Thus, an electronic transmission signal does not fall within any of the four categories of invention. Therefore, Claim 19 is not statutory.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-3, 19, 21 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ayyagari et al (US 2002/0176366) in view of He et al (US 6,088,451).

Claims 1, 19, 21, and 22: Ayyagari et al discloses a system, a data packet, and a computer readable medium for achieving zero-configuration wireless computing comprising:

i. A connection component that can connect a device to a plurality of wireless networks (The approach of the present invention performs automatic network connectivity with the "appropriate" network based on various parameters, as may be set by the user and/or programmatically determined by an application) (paragraphs [0010], [0054]; Fig. 6 step 274); and

ii. A detection component that automatically identifies an encryption type of an available wireless network (the system operates by periodically scanning across all wireless channels to determine currently available infrastructure networks) (paragraph [0011]; Fig. 6 steps 264 and 292), But

does not explicitly disclose that wherein identification of the encryption type is based at least in part upon a failure of a portion of an authentication sequence of the available wireless network or exceeding a time threshold during the authentication sequence of the available wireless network, However, He et al discloses a security system, data packet, and computer readable medium which further discloses wherein identification of the encryption type is based at least in part upon a failure of a portion of an authentication sequence of the available wireless network or exceeding a time threshold during the authentication sequence of the available wireless network (column 31, lines 15-38). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to identify an encryption type based on exceeding a time threshold in Ayyagari et al's disclosure. One would have been motivated to do so in order to automatically providing secure access to network elements as taught by He et al (column 1, lines 5-10).

Claim 2: Ayyagari et al and He et al disclose a system for achieving zero-configuration wireless computing as in claim 1 above, and Ayyagari et al further discloses that identification of the encryption type of the available wireless network by the detection component being based, at least in part, upon receipt of an information element from a wireless network beacon (this preferred channel selection, in one embodiment, is based on appropriate frequency reuse principles and the channels used and received signal strength from beaconing sources)

(paragraphs [0011], [0049], [0059]).

Claim 3: Ayyagari et al and He et al disclose a system for achieving zero-configuration wireless computing as in claim 1 above, and Ayyagari et al further discloses that the available wireless network comprising at least one of an unencrypted network, a Wired Equivalent Privacy (WEP) network requiring a WEP key, a Wi-Fi Protected Access (WPA) encrypted network requiring a WPA pre-shared key, an 802. ix-enabled network that does not support WPA, an 802. ix-enabled network that does support WPA and a wireless provisioning services (WPS) support-enabled network (paragraph [0012]).

10. Claims 4-10, 12, 13, 15-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ayyagari et al (US 2002/0176366) in view of Krantz et al (US 2004/0111520).

Claim 4: Ayyagari et al and He et al discloses a system for achieving zero-configuration wireless computing as in claim 1 above, while neither of them explicitly discloses that the identification the encryption type of the available wireless network by the detection component being based, at least in part, upon iterative probing of the available network. However, Krantz et al discloses an automatic provisioning system, which further discloses that the that the identification by the detection component being based, at least in part, upon iterative probing of the available network (Client 205 may detect available wireless networks, such as, for example, by receiving IEEE 802.11 beacon

frames and/or by sending IEEE 802.11 probe request frames and receiving IEEE 802.11 probe response frames) (paragraph [0066]). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Ayyagari et al and He et al such as to include a step of probing available network. One would have been motivated to do so in order to automatically providing a computer system with appropriate information such that the computer system can be provisioned to communicate on a network as discussed (paragraph [0002]) by Ktantz et al.

Claim 5: Ayyagari et al , He et al and Ktantz et al disclose a system for achieving zero-configuration wireless computing as in claim 4 above, and Ayyagari et al further discloses that the detection component attempts to connect to the available wireless network as a wireless provisioning services-supporting network(the system of the present invention attempts to perform an IEEE 802.11 association with the selected SSID 286) (paragraph [0013]), the detection component determining that the available wireless network is a pre-shared key network if a failure in an authentication sequence from a wireless network beacon is determined (In the event it does not succeed, the system may attempt to associate with other detected infrastructure networks)(paragraphs [0011], [0055]).

Claim 6: Ayyagari et al, He et al and Ktantz et al disclose a system for achieving zero-configuration wireless computing as in claim 5 above, and Ayyagari et al further discloses that the detection component determining that the available

network is a Wi-Fi Protected Access network if a failure in a particular piece of the authentication sequence that identifies a wireless provisioning services supporting network is determined (Fig.3 items 224 and 226).

Claim 7: Ayyagari et al , He et al and Ktantz et al disclose a system for achieving zero-configuration wireless computing as in claim 6 above, and Ktantz et al further discloses that the particular piece of the authentication sequence comprising a type, length value sequence (server 215 can send an EAP Type-Length-Value ("TLV") objects within PEAP to client 205) (paragraphs [0019], [0067], [0079]). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Ayyagari et al and He et al such as to include a type length-value in the authentication sequence. One would have been motivated to do so in order to automatically providing a computer system with appropriate information such that the computer system can be provisioned to communicate on a network as discussed (paragraph [0002]) by Ktantz et al.

Claim 8: Ayyagari et al, He et al and Ktantz et al disclose a system for achieving zero-configuration wireless computing as in claim 6 above, and Ayyagari et al further discloses that the detection component determining that the available network is a wireless provisioning services supporting network if the particular piece of authentication sequence identifying the wireless provisioning services supporting network is received from the wireless network beacon(this preferred channel selection, in one embodiment, is based on appropriate frequency reuse

principles and the channels used and received signal strength from beaconing sources) (paragraphs [0011], [0049], [0059]).

Claim 9: Ayyagari et al and He et al disclose a system for achieving zero-configuration wireless computing as in claim 1 above, while neither of them explicitly discloses that the detection component sends at least one of a connect message, an 802. lx Extensible Authentication Protocol Over LAN (EAPOL) start message, an 802.1x identity message. However, Krantz et al discloses an automatic provisioning system, which further discloses that the detection component sends at least one of a connect message, an 802. lx Extensible Authentication Protocol Over LAN (EAPOL) start message, an 802.1x identity message (computer systems can attempt to authenticate with one another through the transfer of EAP messages (e.g., start messages, response messages, request messages, accept messages, reject messages, etc) (paragraphs [0068], [0069], [0071]). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Ayyagari et al and He et al such as to send at least one connect message, a start message. One would have been motivated to do so in order to automatically providing a computer system with appropriate information such that the computer system can be provisioned to communicate on a network as discussed (paragraph [0002]) by Ktantz et al.

Claim 10: Ayyagari et al and He et al disclose a system for achieving zero-configuration wireless computing as in claim 1 above, while neither of them

explicitly discloses that the detection component receives at least one of an associated message, an 802. 1x identity request message, an authentication message and a provisioning message from a wireless network beacon. However, Krantz et al discloses an automatic provisioning system, which further discloses that the detection component receives at least one of an associated message, an 802. 1x identity request message, an authentication message and a provisioning message from a wireless network beacon (access point 209 can detect that the connection is active and can send an EAP-Request/Identity message to client 205) (paragraph [0073]). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Ayyagari et al and He et al such as to send at least one connect message, a start message. One would have been motivated to do so in order to automatically providing a computer system with appropriate information such that the computer system can be provisioned to communicate on a network as discussed (paragraph [0002]) by Ktantz et al.

Claim 12: Ayyagari et al discloses a method for achieving zero-configuration wireless computing comprising:

i. Attempting to connect to a wireless network as a wireless provisioning services supporting network The approach of the present invention performs automatic network connectivity with the "appropriate" network based on various parameters, as may be set by the user and/or

programmatically determined by an application) (paragraphs [0010], [0054]; Fig. 6 step 274);

ii. Automatically identifying the encryption type of the wireless network (paragraph [0011]; Fig. 6 steps 264and 292), but does not explicitly disclose that wherein identification of the encryption type is based at least in part upon a failure of a portion of an authentication sequence of the available wireless network or exceeding a time threshold during the authentication sequence of the available wireless network, However, He et al discloses a method which further discloses wherein identification of the encryption type is based at least in part upon a failure of a portion of an authentication sequence of the available wireless network or exceeding a time threshold during the authentication sequence of the available wireless network (column 31, lines 15-38).

While neither of them explicitly discloses a step of prompting for a wired equivalent privacy key, if the attempt was not successful. However, Krantz et al discloses an automatic provisioning system, which further discloses a step of prompting for a wired equivalent privacy key, when the attempt was not successful (Through the use of beacon and probe frames client 205 can also detect other configuration settings of an access point, such as, for example supported types of encryption (e.g., Wire Equivalent Protection ("WEP") or Temporal Key Integrity Protocol ("TKIP"))(paragraph [0066]). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention

was made to modify the combined teaching such Ayyagari et al and He et al as to prompt the user for WEP key. One would have been motivated to do so in order to automatically providing a computer system with appropriate information such that the computer system can be provisioned to communicate on a network as discussed (paragraph [0002]) by Ktantz et al.

Claim 13: Ayyagari et al , He et al and Ktantz et al disclose a method for achieving zero-configuration wireless computing as in claim 12 above, and Ayyagari et al further discloses:

i. Waiting up to a threshold period of time for a particular piece of authentication information that identifies a wireless provisioning services supporting network (In the event it does not succeed, the system may attempt to associate with other detected infrastructure networks) (paragraphs [0011], [0051], [0055]);

determining whether the particular piece of authentication information has been received sequence (In the event it does not succeed, the system may attempt to associate with other detected infrastructure networks) (paragraphs [0011], [0051], [0055]);

ii. Identifying the wireless network as a wireless provisioning services supporting network, if the particular piece of authentication information has been received (If this option is selected, the user thereafter may select the authentication method, e.g., EAP-TLS, EAP-MD5, or EAP-MSCHAP (via, e.g., a pull-down menu) to be used. When this authentication option

setting is set, the STA will preferably use the IEEE 802.11 open authentication mode) (paragraph [0042].

Ktantz et al further discloses a step of identifying the wireless network as a Wi-Fi Protected Access (WAP) network, if the particular piece of authentication information has not been received (The defined "WPA" element (line 24) can be included in a configuration file to indicate that authentication is performed in accordance with WiFi Protected Access) (paragraph [0094]). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Ayyagari et al and He et al such as to identify the network as a WPA network. One would have been motivated to do so in order to automatically providing a computer system with appropriate information such that the computer system can be provisioned to communicate on a network as discussed (paragraph [0002]) by Ktantz et al.

Claim 15: Ayyagari et al discloses a method facilitating wireless network detection comprising:

i. Determining whether a wireless network supports 802. 1x, based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence (In the event it does not succeed, the system may attempt to associate with other detected infrastructure networks) (paragraphs [0011], [0051], [0055]);

ii. Determining whether the wireless network supports wireless provisioning services(In the event it does not succeed, the system may

attempt to associate with other detected infrastructure networks) (paragraphs [0011], [0051], [0055]); But does not explicitly disclose that wherein identification of the encryption type is based at least in part upon a failure of a portion of an authentication sequence of the available wireless network or exceeding a time threshold during the authentication sequence of the available wireless network, However, He et al discloses a security system, method, data packet, and computer readable medium which further discloses wherein identification of the encryption type is based at least in part upon a failure of a portion of an authentication sequence of the available wireless network or exceeding a time threshold during the authentication sequence of the available wireless network (column 31, lines 15-38).

While neither of them explicitly discloses a step of Identifying the wireless network as an wired equivalent privacy network requiring a wired equivalent privacy key, when the wireless network does not support 802. 1x, or a step of identifying the wireless networks as an 802.1x network, when the wireless network does not supporting wireless provisioning services or a step of Identifying the wireless network as a wireless provisioning services supporting network, if the wireless network supports wireless provisioning services. However, Krantz et al discloses an automatic provisioning system, which further discloses

i. Identifying the wireless network as an wired equivalent privacy network requiring a wired equivalent privacy key, when the wireless network does not support 802. 1x (the defined "Non802.1XURL" element (line 50) can be included in a configuration sub-file to indicate a URL that can be accessed for Non-802.1X authentication) (paragraph [0098]).

ii. Identifying the wireless network as an 802. 1x network, when the wireless network does not supporting wireless provisioning services (the defined "Open" element (line 22) can be included in a configuration sub-file to indicate open authentication. That is, authentication does not use a pre-shared key required to authenticate with an access point) (paragraph [0094]); and

ii. Identifying the wireless network as a wireless provisioning services supporting network, when the wireless network supports wireless provisioning services The defined "Open" element (line 22) can be included in a configuration sub-file to indicate open authentication. That is, authentication does not use a pre-shared key required to authenticate with an access point) (paragraph [0094]).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the teaching of Ayyagari et al and He et al such as to identify the wireless networks type. One would have been motivated to do so in order to automatically providing a computer system with

appropriate information such that the computer system can be provisioned to communicate on a network as discussed (paragraph [0002]) by Ktantz et al.

Claim 16: Ayyagari et al He et al and Ktantz et al disclose a method for achieving zero-configuration wireless computing as in claim 15 above, and Ktantz et al further discloses that the method comprising at least one of the following acts:

i. Determining whether the wireless networks is encryption enabled (the defined encryption element (lines 29-39) further defines the types of encryption that may be supported by a network) (paragraph [0095]);

ii. Determining whether the wireless network is a Wi-Fi Protected Access (WAP) network (the defined "WPA" element (line 24) can be included in a configuration file to indicate that authentication is performed in accordance with WiFi Protected Access) (paragraph [0094]);

and,

iii. Determining whether the wireless network is a Wi-Fi Protected Access (WAP) pre-shared key network (the defined "WPAPSK" element (line 25) can be included in a configuration sub-file to indicate that authentication is performed in accordance with WiFi Protected Access-Pre-Shared Key authentication) (paragraph [0094]);

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the teaching of Ayyagari et al and He et al such as to identify the wireless networks type. One would have been

motivated to do so in order to automatically providing a computer system with appropriate information such that the computer system can be provisioned to communicate on a network as discussed (paragraph [0002]) by Ktantz et al.

Claim 17: Ayyagari et al, He et al and He et al and Ktantz et al disclose a method for achieving zero-configuration wireless computing as in claim 16 above, and Ktantz et al further discloses that the method further comprising at least one of the following acts:

i. Identifying the wireless network as unencrypted, if the wireless network is not encryption enabled (paragraph [0098]); and,

ii. Identifying the wireless network as a Wi-Fi Protected Access pre-shared key network (The defined "WPA" element (line 24) can be included in a configuration file to indicate that authentication is performed in accordance with WiFi Protected Access) (paragraph [0094]).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the teaching of Ayyagari et al and He et al such as to identify the wireless networks type. One would have been motivated to do so in order to automatically providing a computer system with appropriate information such that the computer system can be provisioned to communicate on a network as discussed (paragraph [0002]) by Ktantz et al.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Chiu Auto-detection of wireless network accessibility US 2003/0204748.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
Friday October 26th, 2007

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136